L Number	Hits	Search Text	DB	Time stamp
1	11	(firewall or proxy) same (authentica$6) same ((back-end or backend) adj2 server)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/05 18:16
2	40	(firewall or proxy) same (authentica$6) same ((back-end or backend))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/05 18:16

proxy server

Last modified: Monday, December 01, 2003

A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Proxy servers have two main purposes:

- **Improve Performance:** Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy server. First user X requests a certain Web page, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the Web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such as Compuserve and America Online, for example, employ an array of proxy servers.
- **Filter Requests:** Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

See the Server Types page in the quick reference section of Webopedia for a comparison of server types.

4/4/04

h eb e c e e h

proxy gateway

<*networking*> A computer and associated software which will pass on a request for a URL from a World-Wide Web browser such as Mosaic to an outside server and return the results. This provides clients that are sealed off from the Internet a trusted agent that can access the Internet on their behalf. Once the client is properly configured, its user should not be aware of the proxy gateway.

A proxy gateway often runs on a firewall machine. Its main purpose is to act as a barrier to the threat of crackers. It may also be used to hide the IP addresses of the computers inside the firewall from the Internet if they do not use official registered network numbers.

Browsers such as Mosaic and Netscape can be configured to use a different proxy or no proxy for each URL access method (or "scheme") - FTP, Gopher, WAIS, news, and HTTP.

Mosaic and proxy gateways.

Compare proxy server.

(1997-06-08)

Try this search on OneLook / Google

Nearby terms: provocative maintenance « prowler « proxy ARP « proxy gateway » Proxy Server » proxy server » PS

4/4/04

h b c c c f c f c cg g e

firewall machine

<*networking*> A dedicated gateway machine with special security precautions on it, used to service outside network, especially Internet, connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind it from crackers. The typical firewall is an inexpensive microprocessor-based Unix machine with no critical data, with modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster. The special precautions may include threat monitoring, call-back, and even a complete iron box keyable to particular incoming IDs or activity patterns.

Firewalls often run proxy gateways.

Synonym flytrap, Venus flytrap.

(1997-06-08)

Nearby terms: firehose syndrome « firewall « firewall code « **firewall machine** » FireWire » fireworks mode » Firmware

4/4/04

h b c c c f c f c cg f e ch e

firewall

Last modified: Thursday, July 24, 2003

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- **Circuit-level gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

9/4/04

h eb e c ff e h